

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

- 1 1. (Currently Amended) A method of using a virtual machine monitor and an operating
2 system on computer hardware in a computer, the method comprising:
3 interposing the virtual machine monitor between the computer hardware and the
4 operating system at runtime, wherein the interposing occurs after booting of the computer; and
5 booting the operating system on the computer hardware before interposing the virtual
6 machine monitor at runtime.
- 1 2. (Cancelled)
- 1 3. (Previously Presented) The method of claim 1, further comprising booting the virtual
2 machine monitor on the computer hardware, booting the operating system on the virtual machine
3 monitor, and devirtualizing the computer hardware before interposing the virtual machine
4 monitor at runtime.
- 1 4. (Previously Presented) The method of claim 1, further comprising devirtualizing the
2 computer hardware after the virtual machine monitor has been interposed.
- 1 5. (Original) The method of claim 1, wherein the computer hardware includes a CPU; and
2 wherein the virtual machine monitor is interposed on the CPU.
- 1 6. (Previously Presented) The method of claim 5, wherein the computer hardware further
2 includes memory, and the virtual machine monitor and the operating system each include CPU
3 interrupt handlers; and wherein interposing the virtual machine monitor on the CPU includes
4 causing privileged instructions to trap to the virtual machine monitor, and redirecting interrupts
5 from the operating system interrupt handlers to the corresponding virtual machine monitor
6 interrupt handlers.

- 1 7. (Original) The method of claim 6, wherein the privileged instructions are caused to trap
2 to the virtual machine monitor by causing the operating system to run at a reduced privilege
3 level; and wherein interposing the virtual machine monitor on the CPU further includes returning
4 control to the operating system at the reduced privilege level.
- 1 8. (Previously Presented) The method of claim 6, wherein the privileged instructions are
2 caused to trap to the virtual machine monitor by using a kernel module of the operating system to
3 reduce a privilege level of the operating system.
- 1 9. (Previously Presented) The method of claim 6, wherein interposing the virtual machine
2 monitor on the CPU further includes disabling physical memory access by the operating system.
- 1 10. ((Currently Amended) The method of claim 6, ~~wherein the computer hardware includes~~
2 ~~memory; and~~ wherein interposing the virtual machine monitor on the CPU further includes
3 loading the virtual machine monitor into the memory.
- 1 11. (Original) The method of claim 10, wherein a kernel module of the operating system is
2 used to allocate memory within the operating system, pin the allocated memory, and load the
3 virtual machine monitor into the pinned memory.
- 1 12. (Original) The method of claim 5, wherein the computer hardware includes memory; and
2 wherein the virtual machine monitor is also interposed on the memory.
- 1 13. (Currently Amended) The method of claim 12, wherein interposing the virtual machine
2 monitor on the memory includes partitioning the memory to provide partitions, and giving the
3 virtual machine monitor access to at least one of the partitions.

- 1 14. (Original) The method of claim 12, wherein interposing the virtual machine monitor on
2 the memory includes using a kernel module of the operating system to allocate a block of the
3 memory, pin the block to prevent the operating system from using the block, and allocate the
4 pinned block to the virtual machine monitor.
- 1 15. (Previously Presented) The method of claim 12, wherein interposing the virtual machine
2 monitor on the memory includes commencing using the virtual machine monitor at runtime to
3 manage memory translation.
- 1 16. (Original) The method of claim 5, wherein the computer hardware includes an I/O
2 device, and wherein the virtual machine monitor is also interposed on the I/O device.
- 1 17. (Previously Presented) The method of claim 16, wherein the operating system includes a
2 dual-mode driver that performs direct hardware control in a first mode and communicates with a
3 device driver of the virtual machine monitor in a second mode; and wherein interposing the
4 virtual machine monitor on the I/O device includes setting the dual-mode driver to the second
5 mode; and redirecting I/O interrupts from interrupt handlers in the operating system to interrupt
6 handlers in the virtual machine monitor.
- 1 18. (Previously Presented) The method of claim 16, wherein interposing the virtual machine
2 monitor on the I/O device includes commencing I/O emulation of the I/O device at runtime.
- 1 19. (Currently Amended) A method of using a virtual machine monitor and an operating
2 system on virtualized computer hardware, the method comprising devirtualizing the virtualized
3 computer hardware at runtime of a computer containing the virtualized computer hardware,
4 wherein runtime includes a period of execution in the computer after boot and before shutdown.
- 1 20. (Previously Presented) The method of claim 19, wherein the virtualized computer
2 hardware includes a CPU; and wherein the CPU is devirtualized at runtime.

1 21. (Previously Presented) The method of claim 20, wherein the virtualized computer
2 hardware further includes physical memory, and the virtual machine monitor and the operating
3 system each include CPU interrupt handlers; and wherein devirtualizing the CPU includes
4 redirecting interrupts from the virtual machine monitor interrupt handlers to the corresponding
5 operating system interrupt handlers.

1 22. (Original) The method of claim 21, wherein devirtualizing the CPU further includes
2 restoring privilege level of the operating system.

1 23. (Previously Presented) The method of claim 21, wherein devirtualizing the CPU further
2 includes enabling physical memory access by the operating system.

1 24. (Previously Presented) The method of claim 21, wherein devirtualizing the CPU further
2 includes unloading the virtual machine monitor from the physical memory.

1 25. (Previously Presented) The method of claim 19, wherein the virtualized computer
2 hardware includes memory; and wherein the memory is devirtualized at runtime.

1 26. (Original) The method of claim 25, wherein memory was allocated from the operating
2 system to the virtual machine monitor during virtualization of the memory; and wherein
3 devirtualizing the memory includes returning the allocated memory to the operating system.

1 27. (Previously Presented) The method of claim 25, wherein devirtualizing the memory
2 includes remapping physical memory and using the operating system to manage address
3 translation with respect to the devirtualized memory.

1 28. (Previously Presented) The method of claim 19, wherein the virtualized computer
2 hardware includes an I/O device, and wherein the I/O device is devirtualized at runtime.

29. (Currently Amended) The method of claim 28, wherein the operating system includes a dual-mode driver that performs direct hardware control in a first mode and communicates with a device driver of the virtual machine monitor in a second mode; and wherein devirtualizing the I/O device includes setting the dual-mode driver to the first mode₂[[;]] and redirecting I/O interrupts from handlers in the virtual machine monitor to handlers in the operating system.

30. (Original) The method of claim 28, wherein devirtualizing the I/O device includes ceasing emulation of the I/O device at runtime.

31. (Currently Amended) A computer comprising hardware, the hardware including memory, the memory encoded with an operating system, a virtual machine monitor, and code means for interposing the virtual machine monitor between the operating system and[[on]] the hardware at runtime, wherein the interposing occurs after booting of the computer,
wherein the operating system is to be booted in the computer before interposing the virtual machine monitor.

32. (Currently Amended) The computer of claim 31, wherein the hardware further includes a CPU, and the virtual machine monitor and the operating system each include CPU interrupt handlers; and wherein the interposing code is to cause ~~means causes~~ privileged instructions to trap to the virtual machine monitor, and to redirect ~~redirects~~ interrupts and traps from the operating system interrupt handlers to the corresponding virtual machine monitor interrupt handlers, whereby the virtual machine monitor is interposed on the CPU at runtime.

33. (Currently Amended) The computer of claim 32, wherein the interposing code is to cause ~~means causes~~ privileged instructions to trap to the virtual machine monitor by causing the operating system to run at a reduced privilege level; and wherein the interposing code is to ~~reduce means reduces~~ a privilege level of the operating system after redirecting the interrupts, and to return ~~returns~~ control to the operating system at the reduced privilege level.

1 34. (Currently Amended) The computer of claim 32, wherein the interposing code means
2 includes a kernel module of the operating system for reducing a privilege level of the operating
3 system, whereby the privileged instructions trap to the virtual machine monitor.

1 35. (Currently Amended) The computer of claim 32, wherein the interposing code is to
2 disable ~~means disables~~ physical memory access by the operating system.

1 36. (Currently Amended) The computer of claim 31, wherein the interposing code means
2 includes a kernel module of the operating system for allocating a block of the memory, pinning
3 the block to prevent the operating system from using the block, and allocating the pinned block
4 to the virtual machine monitor, whereby the virtual machine monitor is interposed on the
5 memory at runtime.

1 37. (Currently Amended) The computer claim 31, wherein the interposing code is to
2 commence ~~means commences~~ using the virtual machine monitor at runtime to manage memory
3 translation, whereby the virtual machine monitor is interposed on the memory at runtime.

1 38. (Currently Amended) The computer of claim 31, wherein the hardware further includes
2 an I/O device; and wherein the interposing code means includes an operating system dual-mode
3 driver to perform ~~that performs~~ direct hardware control in a first mode and to communicate
4 ~~communicates~~ with a device driver of the virtual machine monitor in a second mode; and
5 wherein the interposing code is to set ~~means sets~~ the dual-mode driver to the second mode, [[;]]
6 and to direct ~~redirects~~ I/O interrupts from interrupt handlers in the operating system to interrupt
7 handlers in the virtual machine monitor, whereby the virtual machine monitor is interposed on
8 the I/O device at runtime.

1 39. (Currently Amended) The computer of claim 31, wherein the hardware further includes
2 an I/O device; and wherein the operating system includes a dual-mode driver to perform~~that~~
3 ~~performs~~ direct hardware control in a first mode and to communicate~~communicates~~ with a device
4 driver of the virtual machine monitor in a second mode; and wherein the interposing code is to
5 set~~means sets~~ the dual-mode driver to the second mode,[[;]] and to redirect~~redirects~~ I/O
6 interrupts from interrupt handlers in the operating system to interrupt handlers in the virtual
7 machine monitor, whereby the virtual machine monitor is interposed on the I/O device.

1 40. (Currently Amended) The computer of claim 31, wherein the hardware further includes
2 an I/O device; and wherein the interposing code is to commence~~means commences~~ I/O
3 emulation of the I/O device at runtime, whereby the virtual machine monitor is interposed on the
4 I/O device at runtime.

1 41. (Currently Amended) A computer comprising hardware, the hardware including memory,
2 the memory encoded with code means for virtualizing the hardware, and code means for
3 devirtualizing the hardware at runtime, wherein runtime includes a period of execution in the
4 computer after boot and before shutdown.

1 42. (Currently Amended) The computer of claim 41, wherein the hardware further includes a
2 CPU; and wherein the devirtualizing code is to devirtualize~~means devirtualizes~~ the CPU at
3 runtime.

1 43. (Currently Amended) The computer of claim 42, wherein the memory is further encoded
2 with an operating system including interrupt handlers; wherein the virtualizing code means
3 includes interrupt handlers; and wherein the devirtualizing code is to redirect~~means redirects~~
4 interrupts from the interrupt handlers of the virtualizing code means to the corresponding
5 interrupt handlers of the operating system.

1 44. (Currently Amended) The computer of claim 43, wherein the devirtualizing code is to
2 restore~~means restores~~ privilege level of the operating system.

1 45. (Currently Amended) The computer of claim 43, wherein the devirtualizing code is to
2 enable ~~means enables~~ physical memory access by the operating system.

1 46. (Currently Amended) The computer of claim 41, wherein the devirtualizing code is to
2 devirtualize ~~means devirtualizes~~ the memory at runtime.

1 47. (Currently Amended) The computer of claim 46, wherein the virtualizing code is to
2 allocate ~~means allocates~~ memory from an operating system to the virtualizing means; and
3 wherein the devirtualizing code is to return ~~means returns~~ the allocated memory to the operating
4 system.

1 48. (Currently Amended) The computer of claim 46, wherein the devirtualizing code is to
2 remap ~~means remaps~~ physical memory and to use ~~[[uses]]~~ an operating system to manage address
3 translation with respect to the devirtualized memory.

1 49. (Currently Amended) The computer of claim 41, wherein the hardware includes an I/O
2 device, wherein the virtualizing code is to virtualize ~~means virtualizes~~ the I/O device; and
3 wherein the devirtualizing code is to devirtualize ~~means devirtualizes~~ the I/O device at runtime.

1 50. (Currently Amended) The computer of claim 49, wherein the memory is further encoded
2 with an operating system including dual-mode drivers to ~~[[that]]~~ perform direct hardware control
3 in a first mode and communicate with device drivers of the virtualizing code ~~means~~ in a second
4 mode; and wherein the devirtualizing code is to set ~~means sets~~ the dual-mode drivers to the first
5 mode, ~~[[;]]~~ and to redirect ~~redirects~~ I/O interrupts from handlers in the virtualizing code ~~means~~ to
6 handlers in the operating system.

1 51. (Currently Amended) The computer of claim 49, wherein the devirtualizing code is to
2 cease ~~means ceases~~ emulation of the I/O device at runtime.

1 52. (Currently Amended) An article for use with an operating system on computer hardware,
2 the article comprising a computer-readable storage medium storing ~~containing~~ software that
3 when executed by a computer causes the computer to virtualize at least a portion of the computer
4 hardware at runtime by providing a virtual machine monitor between the operating system and
5 the computer hardware, wherein the virtualizing occurs after boot of the computer and loading of
6 the operating system, and
7 wherein the operating system is to be booted in the computer before virtualizing the at
8 least a portion of the computer hardware at runtime.

1 53. (Currently Amended) The article of claim 52, wherein the computer hardware further
2 includes a CPU, and wherein ~~the computer hardware is virtualized using a virtual machine~~
3 ~~monitor, and~~ the virtual machine monitor and the operating system each include CPU interrupt
4 handlers; and wherein the software is executable to cause ~~causes~~ privileged instructions to trap to
5 the virtual machine monitor, and causes interrupts and traps to be redirected from the operating
6 system interrupt handlers to the corresponding virtual machine monitor interrupt handlers.

1 54. (Currently Amended) The article of claim 53, wherein the software is executable to cause
2 ~~causes~~ the privileged instructions to trap to the virtual machine monitor by reducing a privilege
3 level of the operating system, and wherein the software causes control to be returned to the
4 operating system at the reduced privilege level.

1 55. (Currently Amended) The article of claim 53, wherein the software is executable to cause
2 ~~causes~~ physical memory access by the operating system to be disabled.

1 56. (Currently Amended) The article of claim 52, wherein the computer hardware includes
2 memory, and wherein the ~~software includes a virtual machine monitor~~ is for causing a kernel
3 module of the operating system to allocate a block of the memory, pin the block to prevent the
4 operating system from using the block, and allocate the pinned block to the virtual machine
5 monitor.

1 57. (Currently Amended) The article of claim 52, wherein the ~~software includes a virtual~~
2 machine monitor is to manage ~~that manages~~ memory translation at runtime.

1 58. (Currently Amended) The article of claim 52, wherein the computer hardware further
2 includes an I/O device; and wherein the software includes an operating system dual-mode driver
3 ~~that performs~~ to perform direct hardware control in a first mode and ~~communicate~~communicates
4 with a corresponding device driver of a virtual machine monitor in a second mode; and wherein
5 the dual-mode driver is set to the second mode when the at least the portion of the hardware is
6 virtualized, during runtime interposition; and wherein I/O interrupts are redirected from interrupt
7 handlers in the operating system to interrupt handlers in the virtual machine monitor.

1 59. (Currently Amended) The article of claim 52, wherein the computer hardware further
2 includes an I/O device; and wherein the operating system includes a dual-mode driver that to
3 perform ~~performs~~ direct hardware control in a first mode and ~~communicate~~communicates with a
4 device driver of the virtual machine monitor in a second mode; and wherein the dual-mode
5 driver is set to the second mode when the at least the portion of the hardware is
6 virtualized, during interposition; and wherein I/O interrupts are redirected from interrupt handlers
7 in the operating system to interrupt handlers in the virtual machine monitor.

1 60. (Currently Amended) The article of claim 52, wherein the computer hardware further
2 includes an I/O device; and wherein the software is executable to cause ~~causes~~ I/O emulation of
3 the I/O device to commence at runtime.

1 61. (Original) An article for running an operating system and a virtual machine monitor on a
2 computer, the computer including an I/O device, the article comprising computer memory
3 encoded with an I/O driver having first and second modes of operation, the I/O driver operable in
4 the first mode to interface directly between the operating system and the I/O device, the I/O
5 driver operable in the second mode to interface between the operating system and a
6 corresponding I/O driver of the virtual machine monitor.

1 62. (Currently Amended) An article for use with an operating system on computer hardware,
2 the article comprising a computer-readable storage medium storing ~~containing~~ software that
3 when executed by a computer causes the computer to devirtualize at least a portion of virtualized
4 hardware at runtime, wherein runtime is a period of execution in the computer after boot and
5 before shutdown.

1 63. (Previously Presented) The article of claim 62, wherein the virtualized hardware includes
2 a CPU; and wherein the software causes the CPU to be devirtualized at runtime.

1 64. (Previously Presented) The article of claim 63, wherein the virtualized hardware further
2 includes memory, and wherein the memory is further encoded with an operating system
3 including first interrupt handlers; wherein the software includes second interrupt handlers; and
4 wherein the software causes interrupts to be redirected from the second interrupt handlers to the
5 corresponding first interrupt handlers.

1 65. (Original) The article of claim 64, wherein the software causes privilege level of the
2 operating system to be restored.

1 66. (Original) The article of claim 64, wherein the software causes physical memory access
2 by the operating system to be enabled.

1 67. (Previously Presented) The article of claim 62, wherein the virtualized hardware includes
2 a memory, and wherein the software causes the memory to be devirtualized at runtime.

1 68. (Original) The article of claim 67, wherein if a part of the memory was allocated from an
2 operating system to a virtual machine monitor prior to the runtime devirtualization, the software
3 causes the allocated memory to be returned to the operating system as part of the runtime
4 devirtualization.

1 69. (Previously Presented) The article of claim 67, wherein the software causes physical
2 memory to be remapped and wherein the software allows an operating system to manage address
3 translation with respect to the devirtualized memory.

1 70. (Original) The article of claim 62, wherein the virtualized hardware includes an I/O
2 device; and wherein the software causes the I/O device to be devirtualized at runtime.

1 71. (Previously Presented) The article of claim 70, wherein the virtualized hardware further
2 includes a memory, and wherein the memory is further encoded with an operating system
3 including dual-mode drivers that perform direct hardware control in a first mode and
4 communicate with virtual device drivers in a second mode; and wherein the software causes the
5 dual-mode drivers to be set to the first mode.

1 72. (Original) The article of claim 70, wherein the software causes emulation of the I/O
2 device to cease at runtime.